Examiner's Objections

Examiner states that :

(I)   Applicant contends that the method of delivery of email by the independent third party to the intended recipient in the pending application is not the same as disclosed by Epstein. Examiner cites prior art: US PN 6, 023, 510 issued to Epstein, in addition to US Publication Number 2002/01291098 (Sykes) and US PN 6,081,899 (Byrd).

(II) Applicant contends that the method of identifying the e-mail source of the re-mailer and the email address of the intended recipient in the pending application is not the same as disclosed by Epstein.

(III)   Applicant contends that Epstein does not disclose method of retrieval of the email by the intended recipient in the pending application.

(IV)   Applicant contends that Epstein does not disclose the method of posting a reply by the intended recipient in the pending application.

In considering (I), Applicant contends that the method of identifying the e-mail source of the re-mailer in the pending application is not the same as disclosed by Epstein. Applicant respectfully traverses.

In considering (II), Applicant contends that the method of identifying the e-mail source of the re-mailer in the pending application is not the same as disclosed by Epstein. Examiner asserts that Epstein was cited so as to disclose the convention operation of anonymous re-mailer systems to be well known in the art at the time of the invention, and not to teach the specific embodiments of Epstein's invention. Therefore, Applicant's arguments that pertain to the

particular functionality (i.e., random sequence number or a public bulletin board whereby all of the parties remain anonymous) of the anonymous query system of Epstein is not relevant. Furthermore, Epstein discloses that the first originator of the email is anonymous to the final recipient but is known to the provider (i.e., remailer retains the source addresses of the message originator's column 1, lines 58-60), which is equivalent to the functionality of Applicant's claimed invention. Applicant respectfully traverses.

In considering (III), Applicant contends that Epstein does not disclose method of retrieval of the email by the intended recipient in the pending application. Examiner asserts that Epstein was cited so as to disclose the convention operation of anonymous re-mailer systems to be well known in the art at the time of the invention, and not to teach the specific embodiments of Epstein's invention. Therefore, Applicant's arguments that pertain to the particular functionality (i.e., public key or PKI) of the anonymous query system of Epstein is not relevant. Applicant respectfully traverses.

In considering (IV), Applicant contends that Epstein does not disclose the method of posting a reply by the intended recipient in the pending application. Examiner asserts that Epstein was cited so as to disclose the convention operation of anonymous re-mailer systems to be well known in the art at the time of the invention, and not to teach the specific embodiments of Epstein's invention. Therefore, Applicant's arguments that pertain to the particular functionality (i.e., public key or PKI) of the anonymous query system of Epstein is not relevant. Applicant respectfully traverses.

Applicant reiterates its position with respect to Epstein. Applicant addresses the Examiner's objections with respect to Sykes, Byrd and Epstein in turn. Applicant respectfully traverses on the following basis:

CLAIM REJECTIONS UNDER 35 U.S.C. § 103

OBVIOUSNESS

U.S.C.§ 103 ANALYSIS

CLAIMS 46-48 AND 50-52 IN VIEW OF EPSTEIN

ANALYSIS OF EPSTEIN SPECIFICATION, AS REFERENCED AND CITED BY THE EXAMINER IN THE OFFICE ACTION

In considering (I), Applicant contends the method of delivery of email by the independent third party to the intended recipient in the pending application is not the same as disclosed by Epstein. Examiner asserts that Epstein was cited so as to disclose the convention operation of anonymous re-mailer systems to be well known in the art at the time of the invention, and not to teach the specific embodiments of Epstein's invention. Therefore, Applicant's arguments that pertain to the particular functionality (i.e., public key or PKI) of the anonymous query system of Epstein is not relevant. Examiner states that Epstein expressly discloses the well know [sic] use of an anonymous remailer which provides: service request comprising that the client's identity be withheld from the intended recipient; the processing unit resending the electronic message to the intended

recipient as identified by the client in the registration account; the processing unit notifying the intended recipient that the electronic message has been sent on behalf of the client by the processing unit (column 1, lines 45-62).[1]

Examiner further states that Epstein shows the method whereby the processing unit clearly identifies a constant and verifiable email address of the processing unit and verifiable contact information of the processing unit , in the email to the intended recipient (i.e. header information which points back to the remailer; column 1, lines 45-62.[2]

Finally, Examiner posits that Epstein shows the method whereby the intended recipient is notified that the intended recipient may choose to post a reply with the processing unit for the originator of the electronic message, (i.e. remailer retains the source address of the message originators for replies to be forwarded, column 1, lines 45-62).[3]

Applicant respectfully traverses and addresses Examiner's objections regarding Epstein in turn. Applicant respectfully submits that the above cited portions of the Epstein specification do not disclose the method of the pending application. Specifically, an analysis of the references to Epstein, as cited by the Examiner, fail to disclose the following novelties of the pending application.

---

[1] Office Action dated September 30th, page 5, paragraph 2 through page 6, paragraph 1.

[2] Office Action dated September 30th, page 9, paragraph 3 through page 10, paragraph 1.

[3] Office Action dated September 30th, page 10, paragraph 2.

1. THE METHOD OF DELIVERY OF THE EMAIL BY THE INDEPENDENT THIRD PARTY TO THE INTENDED RECIPIENT IN THE PENDING APPLICATION IS NOT DISCLOSED BY EPSTEIN

Examiner states in her Office Action[4] that the Epstein abstract discloses the well know [sic] use of an anonymous remailer which provides: service request comprising that the client's identity be withheld from the intended recipient; the processing unit resending the electronic message to the intended recipient as identified by the client in the registration account; the processing unit notifying the intended recipient that the electronic message has been sent on behalf of the client by the processing unit (column 1, lines 45-62).[5]

Applicant references the Epstein specification to further disclose:
The specific use of a public key <u>as the sole means by which an email is posted a public bulletin board</u> to be retrieved by an intended recipient.

Applicant refers to column 2 line 1, through column 4 line 11 with the pertinent references highlighted.

- It is an object of the present invention to provide a method for queries in the form of electronic messages to be submitted securely and anonymously to an information provider via a public network, such as the Internet, and to provide a method for secure responses

---

[4] Application/Control Number 09/982,145, Final Office Action, pp 4-5.

[5] Office Action dated September 30th, page 5, paragraph 2 through page 6, paragraph 1.

by the information provider which are obtainable by the inquiring party.

- Briefly, these and other objects are satisfied by a method, which from the point of view of the user, is for secure anonymous querying of a provider in which:

  a random number sequence, a public key of the user, and a corresponding private key of the user are generated;

  a public key of the provider is used to form an electronic encrypted query package containing information including a query, the generated random number sequence, and the generated public key of the user, the information including an identification of a public bulletin board for posting a message comprising the random number sequence in association with an encrypted response to the query, **and the query package being structured such that the contained information can be obtained by the provider by operations including a decryption with the private key of the provider;** and the query package is sent to the provider via a network in a manner that the user is not identifiable to the provider.

- Still another aspect of the invention from the point of view of the server is **that the query package is constructed in a manner that a first part including at least the query is encrypted using a symmetric key of the user and a second part including at least the symmetric key of the user is encrypted using the public key of the provider,** and the method further comprises decrypting the second part of the query package using the private key of the provider to obtain at least the symmetric key of the user,

and decrypting the first part of the query package using the symmetric key of the user to obtain at least the query.

- The present invention also comprises a stored message on a public bulletin board responsive to an anonymous query, **said message comprising a random number sequence and an associated encrypted electronic response package containing a response to the query**, said response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user.

- Another aspect of the inventive stored message is that the response package is constructed in a manner that a first part including at least the response is encrypted using a symmetric key of the provider and a second part **including at least the symmetric key of the provider is encrypted using a public key of a user who made the anonymous query.**

2. THE METHOD OF IDENTIFYING THE EMAIL ADDRESS SOURCE OF THE REMAILER AND THE EMAIL ADDRESS OF THE INTENDED RECIPIENT IN THE PENDING APPLICATION IS NOT DISCLOSED BY EPSTEIN

Examiner states in her Office Action[6] that the Epstein abstract discloses the well know [sic] use of an anonymous remailer which provides: service request comprising that the client's identity be withheld from the intended recipient; the processing unit resending the electronic message to the intended recipient as

---

[6] Application/Control Number 09/982,145, Final Office Action, pp 4-5.

identified by the client in the registration account; the processing unit notifying the intended recipient that the electronic message has been sent on behalf of the client by the processing unit (column 1, lines 45-62).[7]

The Epstein abstract reads as follows:

- A method for secure anonymous querying by a user of an information provider by electronic mail and for obtaining a reply uses a public key of the provider to form an electronic encrypted query package containing information including a query, **a generated random number sequence, a hash of the query, a generated public key of the user, and an identification of a public bulletin board.**[8]

The prior art cited by Examiner (column 1, lines 45-62) reads as follows: Also, anonymous remailers for electronic mail are known for the purpose of forwarding messages from a message originator to a recipient, with all message header information which could be used to trace the message back to its source replaced by information which just points back to the anonymous remailer. It is possible that the message sent to the remailer for forwarding could be an encrypted one, but the destination address would be in the clear because such remailers are generally not **set up to receive and decrypt an encrypted destination address.** Consequently, an eavesdropper monitoring electronic mail messages sent to a remailer **could determine both actual source and destination addresses**. Also, because the remailer must necessarily retain the source addresses of message originators in order to enable replies to be forwarded, there is the risk that the **source addresses**

---

[7] Office Action dated September 30th, page 5, paragraph 2 through page 6, paragraph 1.

[8] US PN 6,023, 510, abstract.

<u>**could be obtained if the remailer were compromised.**</u>

Applicant references the Epstein specification to further disclose:

That the source and the identity of the originating email address are not in fact identifiable beyond a numeric code associated with a verifiable website. In fact, Epstein discloses a method whereby an anonymous query is posted on a public board and is retrieved anonymously. In fact, the identities of the originator of the email and the public terminal that transmits it, are unknown to the intended recipient beyond a number. <u>Moreover, the method disclosed by Epstein does not involve the resending of an email, rather a public board whereby the parties may interact anonymously as opposed to identifying the sender and the intended recipient.</u>

Applicant refers to column 2 line 1, through column 4 line 11 with the pertinent references highlighted.

- It is an object of the present invention to provide **a method for queries in the form of electronic messages to be submitted securely and anonymously to an information provider via a public network,** such as the Internet, and to provide a method for secure responses by the information provider which are obtainable by the inquiring party.

- Briefly, these and other objects are satisfied by a method, which from the point of view of the user, is for secure anonymous querying of a provider in which:

  a random number sequence, a public key of the user, and a corresponding private key of the user are generated;

  a public key of the provider is used to form an electronic encrypted query package **containing information including a query, the**

generated random number sequence, and the generated public key of the user, the information including an identification of a public bulletin board for posting a message comprising the random number sequence in association with an encrypted response to the query, and the query package being structured such that the contained information can be obtained by the provider by operations including a decryption with the private key of the provider; and

the query package is sent to the provider via a network in a manner that the user is not identifiable to the provider.

- Other aspects of the inventive method from the point of view of the user are that the query package is sent to the provider from a public terminal, and that a hash of the query is generated and is included in the information contained in the query package.

- A further aspect of the present invention is that a symmetric key of the user is generated and the query package is constructed in a manner that a first part including at least the query is encrypted using the generated symmetric key of the user and a second part including at least the generated symmetric key of the user is encrypted using the public key of the provider.

- From the point of view of the information provider, the present invention is directed to a method for secure response by a provider to an anonymous query from a user in which:

an electronic encrypted query package containing information including a query, a random number sequence, and a public key of the user is received via a network, the information

including an identification of a public bulletin board for posting a message comprising the random number sequence in association with an encrypted response to the query, and the query package being structured such that the contained information can be obtained by the provider by operations including a decryption with the private key of the provider;

the private key of the provider is used to obtain the information in said query package;

the public key of the user is used to form an electronic encrypted response package containing a response to the query, said response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user; and

a message comprising the random number sequence in association with the response package is posted to the identified public bulletin board.

- Another aspect of the present invention from the point of view of the server is that a hash of the query is included in the information contained in the query package, and the method further comprises computing a hash of the query, and comparing the computed hash with the hash included in the information.

- Still another aspect of the invention from the point of view of the server is that the query package is constructed in a manner that a first part including at least the query is encrypted using a symmetric key of the user and a second part including at least the symmetric key of the user is encrypted using the public key of the provider,

and the method further comprises decrypting the second part of the query package using the private key of the provider to obtain at least the symmetric key of the user, and decrypting the first part of the query package using the symmetric key of the user to obtain at least the query.

- The present invention also comprises a stored message on a public bulletin board **responsive to an anonymous query, said message comprising a random number sequence and an associated encrypted electronic response package containing a response to the query**, said response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user.

- Another aspect of the inventive stored message is that the response package is constructed in a manner that a first part including at least the response is encrypted using a symmetric key of the provider and a second part including at least the symmetric key of the provider is encrypted **using a public key of a user who made the anonymous query.**

- Other objects, features and advantages of the present invention will become apparent upon perusal of the following detailed description when taken in conjunction with the appended drawing, wherein:

In a first particular embodiment, the present invention includes a method for secure anonymous querying by a user of a provider to whom a public key, private key pair is assigned, the public key of the provider being publicly obtainable by the user, the method comprising: formulating by the user of a query to be sent to the provider, generating by the user of a

random number sequence, a public key of the user, and a
corresponding private key of the user for sole use with said
formulated query; forming an electronic encrypted query package
by the user by operations including encryption with the public
key of the provider obtained by the user, said electronic
encrypted query package containing information including the
formulated query, the generated random number sequence,
the generated public key of the user, and an identification of a
public bulletin board for posting a message comprising the
random number sequence in association with an encrypted
response to the query, and said query package being structured
such that the contained information can be obtained by the provider
by operations including a decryption with the private key of the
provider; and sending by the user of the query package to the
provider via a network in a manner that the user is not
identifiable to the provider, wherein the generated private key
and the generated random number sequence are retained by
the user.

- In a first aspect of the first particular embodiment, the method
  further comprises: receiving by the provider via a network said
  query package sent by the user; obtaining by the provider by
  operations including decryption with the private key of the provider
  the information in said query package; formulating by the provider
  of a response to the query; forming an electronic encrypted
  response package by the provider by operations include
  encryption with the public key of the user contained in said
  query package, said electronic encrypted response package
  containing the formulated response to the query, said response
  package being structured such that the response to the query can
  be obtained by the user by operations including a decryption with

the private key of the user; **posting by the provider of a message comprising the random number sequence in association with the response package to the identified public bulletin board;** accessing the identified bulletin board by the user in order to **download the response package associated with that message posted by the provider including the random number sequence generated by the user;** and obtaining by the user by operations including decryption with the private key of the user of the response information in said response package.

Applicant notes the differences between the prior art cited and the pending application regarding the method of delivery of the email. The method of the pending application does not disclose the use of a random sequence number or a public bulletin board <u>whereby all of the parties remain anonymous</u>. **The method of Epstein specifically discloses that the identity of the user is not known to the provider.** The method of the present invention discloses a method whereby the first originator of an email is anonymous to the final recipient but is known to the provider. Moreover, the method of the present invention discloses a method whereby the remailer is clearly identified and whereby the intended recipient is clearly identified.

3. THE METHOD OF RETRIEVAL OF THE EMAIL BY THE INTENDED RECIPIENT IN THE PENDING APPLICATION IS NOT DISCLOSED BY EPSTEIN

Applicant references the Epstein specification to further disclose:
The specific use of a private key <u>as the sole means by which an email posted on a public bulletin board</u> is used to be retrieved by an intended recipient.

Applicant refers to column 2 line 1, through column 4 line 11 with the pertinent references highlighted.

- It is an object of the present invention to provide a method for queries in the form of electronic messages to be submitted securely and anonymously to an information provider via a public network, such as the Internet, and to provide a method for secure responses by the information provider which are obtainable by the inquiring party.

- Briefly, these and other objects are satisfied by a method, which from the point of view of the user, is for secure anonymous querying of a provider in which:

  a random number sequence, a public key of the user, and a corresponding private key of the user are generated;

  a public key of the provider is used to form an electronic encrypted query package containing information including a query, the generated random number sequence, and the generated public key of the user, **the information including an identification of a public bulletin board for posting a message comprising the random number sequence in association with an encrypted response to the query, and the query package being structured such that the contained information can be obtained by the provider by operations including a decryption with the private key of the provider;** and

  the query package is sent to the provider via a network in a manner that the user is not identifiable to the provider.

- Other aspects of the inventive method from the point of view of the user are that the query package is sent to the provider from a public

terminal, and that a hash of the query is generated and is included in the information contained in the query package.

- A further aspect of the present invention is that a symmetric key of the user is generated and the query package is constructed in a manner that a first part including at least the query is encrypted using the generated symmetric key of the user and a second part including at least the generated symmetric key of the user is encrypted using the public key of the provider.

- From the point of view of the information provider, the present invention is directed to a method for secure response by a provider to an anonymous query from a user in which:

an electronic encrypted query package containing information including a query, a random number sequence, and a public key of the user is received via a network, **the information including an identification of a public bulletin board for posting a message comprising the random number sequence in association with an encrypted response to the query, and the query package being structured such that the contained information can be obtained by the provider by operations including a decryption with the private key of the provider;**

the private key of the provider is used to obtain the information in said query package;

the public key of the user is used to form an electronic encrypted response package containing a response to the query, said **response package being structured such that the response to the query can be obtained by the user by operations including**

a decryption with the private key of the user; and

a message comprising the random number sequence in association with the response package is posted to the identified public bulletin board.

- Another aspect of the present invention from the point of view of the server is that a hash of the query is included in the information contained in the query package, and the method further comprises computing a hash of the query, and comparing the computed hash with the hash included in the information.

- Still another aspect of the invention from the point of view of the server is that the query package is constructed in a manner that a first part including at least the query is encrypted using a symmetric key of the user and a second part including at least the symmetric key of the user is encrypted using the public key of the provider, and the method further comprises decrypting the second part of the query package using the private key of the provider to obtain at least the symmetric key of the user, and decrypting the first part of the query package using the symmetric key of the user to obtain at least the query.

- The present invention also comprises a stored message on a public bulletin board responsive to an anonymous query, said message comprising a random number sequence and an associated encrypted electronic response package containing a response to the query, said response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user.

- Another aspect of the inventive stored message is that the response package is constructed in a manner that a first part including at least the response is encrypted using a symmetric key of the provider and a second part including at least the symmetric key of the provider is encrypted using a public key of a user who made the anonymous query.

- Other objects, features and advantages of the present invention will become apparent upon perusal of the following detailed description when taken in conjunction with the appended drawing, wherein:

In a first particular embodiment, the present invention includes a method for secure anonymous querying by **a user of a provider to whom a public key, private key pair is assigned, the public key of the provider being publicly obtainable by the user, the method comprising: formulating by the user of a query to be sent to the provider, generating by the user of a random number sequence, a public key of the user, and a corresponding private key of the user for sole use with said formulated query;** forming an electronic encrypted query package by the user by operations including encryption with the public key of the provider obtained by the user, said electronic encrypted query package containing information including the formulated query, the generated random number sequence, the generated public key of the user, and an identification of a public bulletin board for posting a message comprising the random number sequence in association with an encrypted response to the query, and said query package being structured such that the contained information can be obtained by the provider **by operations including a decryption with the private key of the provider; and sending by the user of**

the query package to the provider via a network in a manner that the user is not identifiable to the provider, wherein the generated private key and the generated random number sequence are retained by the user.

- In a first aspect of the first particular embodiment, the method further comprises: receiving by the provider via a network said query package sent by the user; obtaining by the provider by operations including decryption with the private key of the provider the information in said query package; formulating by the provider of a response to the query; **forming an electronic encrypted response package by the provider by operations include encryption with the public key of the user contained in said query package, said electronic encrypted response package containing the formulated response to the query,** said response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user; posting by the provider of a message comprising the random number sequence in association with the response package to the identified public bulletin board; **accessing the identified bulletin board by the user in order to download the response package associated with that message posted by the provider including the random number sequence generated by the user; and obtaining by the user by operations including decryption with the private key of the user of the response information in said response package.**

Applicant notes the differences between the prior art cited and the pending application regarding the method of retrieval of the email. The method of the pending application does not disclose the use of a public key or PKI as a

means to retrieve an email for an intended recipient from a public bulletin board.

4. THE METHOD OF POSTING A REPLY BY THE INTENDED RECIPIENT IN THE PENDING APPLICATION IS NOT DISCLOSED BY EPSTEIN

Applicant references the Epstein specification to further disclose:
The specific use of a private key as the sole means by which a reply/response email is posted to a public bulletin board to be retrieved by an intended recipient.

U.S.C.§ 103 ANALYSIS

CLAIMS 46-48 AND 50-52 IN VIEW OF SYKES

In the Office Action, Examiner states[9]: that in reference to claims 46-48 and 50-52, Sykes discloses a method and system for archiving, registering, and verifying electronic communications transmitted between clients and recipients via a network (i.e. internet), (abstract and paragraph [0004], lines 1-13). Specifically, Examiner states that Sykes discloses the third party archiving and verification system to comprise: [10]

- The method for registering and certifying an electronic message, the system and method further comprising a client, an intended recipient, a

---

[9] Application/Control Number 09/982,145, Office Action, pp 3-4.

[10] Application/Control Number 09/982,145, Office Action, pp 3-4.

website (i.e. third party archiving and verification website, Figures 4-22), a processing unit (i.e. third party archiving and verification server), an email database, a means (i.e. third party archiving and verification provider) to register the electronic message, the system and method, (abstract; paragraph [0004], lines 1-13; and paragraph [0038], line 1 to paragraph [0040], line 17), comprising the steps of:

- The client accessing the website and establishing a registration account; the processing unit assigning a code (i.e. account ID) to the registration account of the client, (paragraph [0048], line 1 to paragraph [0049], line 16 and Figure 4); and

- The processing unit receiving the electronic message, the electronic message being from the client; the processing unit storing information about the electronic message and the registration account in the email database; the **processing unit resending the electronic message to the intended recipient as identified by the client in the registration account**; the processing unit tracking the date the electronic message was sent by the processing unit; the processing unit tracking the date the electronic message was received by the intended recipient; the processing unit creating a confirmation record (i.e. message table entry) that comprises the date the electronic message was sent

and the date the electronic message was received by the intended recipient; the processing unit sending the client a copy of the confirmation record (Figure 26); and the processing unit storing information about the confirmation record and the registration account in the email database, (paragraph [0038], line 1 to [0047], line 12; paragraph [0059], line 1 to paragraph [0061], line 8; and paragraph [0065], lines 9-13).

Applicant argues that the above cited method Examiner states is disclosed in Sykes is not analogous to the method disclosed in the PENDING application, as amended in the second response to the Final Office Action. In fact, Applicant notes that the references to Sykes, as cited above, by the Examiner reads precisely as follows in the Sykes specification:

- A method and system for archiving and/or verifying electronic communications. The method and system provide verification of an email sent by a sender to a recipient, comprising receiving a copy of an email as an addressee; indexing the email according to at least one of sender, recipient, date, or subject matter; **and storing an exact copy of the email as received**. The method and system also provide for secure electronic communication between a sender and at least one recipient, comprising receiving from the sender view a secure internet connection a message and the email

address of at least one intended recipient of the message; **sending an email message to the at least one intended recipient of the message that a <u>message is waiting</u>**; transmitting the message to the at least one intended recipient via a secure internet connection established by the at least one intended recipient; **and sending an email message to the sender that the at least one recipient has been sent the message**. The method and system also provide for transmitting a facsimile for a sender to a recipient, the comprising: receiving an electronic facsimile message from the sender together with the facsimile number of the recipient; storing a copy of the electronic facsimile message; transmitting the facsimile message to the facsimile number of the recipient. [11]

- This invention relates to archiving and/or verifying electronic communications. According to a first aspect of the invention relating to sending verifiable email messages, the invention comprises addressing the email to a third party verification provider, either as an addressee or as a cc, who will index the message according to at least one of sender, date, recipient, and subject, and store an exact copy of the e-mail message. Similarly, the invention also relates to providing **email verification** of an email sent by a sender to a recipient, **comprising receiving a copy of an email as an**

---

[11] Sykes abstract, US publication number 2002/0129108, as cited by Examiner in the Final Office Action, page 4, paragraph 3.

addressee; indexing the email according to at least one of sender, recipient, date, or subject matter; and storing an exact copy of the email as received.[12]

- According to a first aspect, this invention relates to a **system and a method for senders to backup and archive email to a third party server without the need for conventional backup software, thereby providing proof of on-line communications.** The system and method are preferably implemented by a third party archiving and verification provider using an Application Service Provider ("ASP") model that allows a sender to use the system and method regardless of his or her location on the Internet. An example of the structure of tables in a SQL database for implementing the system and method of this invention is shown in Appendix A, attached hereto, and incorporated herein by reference. In the preferred embodiment, no special software is required, and an email sender can use the system without changing his standard email process.

Referring to FIG. 1, at 22 the sender sends an email to the recipient, and to the third party archiving and verification provider

---

[12] Sykes specification, paragraph 004, US publication number 2002/0129108, as cited by Examiner in the Final Office Action, page 4, paragraph 3.

either as an addressee (via the "To:" field) or as a copy (via the "CC:" field). Using any conventional email program, such as Outlook, Lotus Notes, Eudora, etc., the sender prepares an email to a recipient, and in the "To" field, or in the "CC:" field also addresses the email to the sender's account with the third party archiving and verification provider. For example an email sender would address the email, or copy the email, to his or her system account xxxxx@yyyyy.com, where xxxxx is a string identifying the sender's account with the third party archiving and verification provider, and where yyyyy.com is the third-party verification provider's email address.

At 24, the email message is received by the third party archiving and verification provider. At 26, a Message Transfer Agent (MTA), for example Sendmail, available from Sendmail, Emoryville, Calif., passes the email to a filter that generates an id based upon the time and date of receipt. The MTA is running on the system server. The email's id is preferably a 24 character identification code in the format yyyymmddhhmmssnnnnnnnnnn where yyyymmdd is an eight-character representation of the date of receipt, hhmmss is a six-character representation of the time of receipt, and nnnnnnnnnn is a unique ten-digit integer. At 28, the email message is written out to a queue directory based upon the id assigned to the email. At 30,

a record is inserted into a queue table in the system's database, which cues a cataloging daemon to begin processing the message. At 32 the MTA returns to processing incoming mail requests.[13]

• The third party verification provider's system includes at least one, and preferably more than one, cataloging daemons that monitor the queue table in the system database. The cataloging daemons also run on the system server. The number of cataloging daemons depends upon the CPU and the IO. Each cataloging daemon is assigned an id that corresponds to the queue table and the queue directories. The queue table has 2 fields: a queue number and a queue message ID. The queue directory is structured as: /gp/gpc1/outgoing, /gp/gpc1/incoming, /gp/gpc0/outgoing, and /gp/gpc0/incoming, and depending on the number of queues desired, the gpc(number) directory would be correspondingly increased. The same applies for an outgoing queue; a single process is in charge of it as well. When a cataloging daemon encounters an entry in its queue, it begins processing.

At 34, the header of the email message is read, based on RFC-822 internet mail standards, (which standards are incorporated

---

[13] Sykes specification, US publication number 2002/0129108, paragraph 38, line 1, to paragraph 40, line 17.

herein by references as if fully set forth). At 36, each email address in the "To:" and "CC:" lines of the email message's header are temporarily stored in an array, which may be a simple character pointer array. The "From:" line of the email message's header is temporarily stored separately. At 38, the cataloging daemon performs a lookup in an alias table of each email address to determine if that email address is a system account with the third party archiving and verification provider. If an email address is an account on the system, the cataloging daemon extracts the system's id for that account. At 40, if the address is valid, the email message's "Received:" header is verified with the MTA table. The MTA table is an extra security feature that stores and allows comparison with the mail relay authorized to deliver the email message to the account. This is an optional feature, that is preferably turned off by default for most accounts. The MTA table has 2 fields, user ID and the sender's MTA's host name. This ensures that the email message was sent from the proper internet mail relay, i.e. an email address that, according to the user's account profile, is authorized to send email to the account. At 42, if the internet mail relay is correct or if it is non-existent the cataloging daemon checks the email message's "From:" header against the address table to verify that the address is allowed to send to the system account. "Non-existent" means that no record is found in

the MTA table for that user. This means that the user did not wish to restrict email coming in based on their outgoing mail server. If the user does have an entry and that entry does not match the value in the MTA table, the message is rejected and an error email is placed in the queue for delivery to the user who sent the email. At 44, if the operations at 38, 40 and 42 are successful, the email message is passed to a catalogue routine, which is part of the cataloging daemon. If there is an error, appropriate error routines are called.

At 46, the email message's "To:", "From:", and "Subject:" lines and the message's size are stored in the system's message table, with the email message referred to by its assigned message id. The message table has the following fields: a) message id; b) user id; c) folder id (for later use in grouping messages); d) "To:" line; e) "From:" line; f) "Subject:" line; g) "Date:" line; h) "Time:" line; i) "Size:" line; j) expiration date; and k) has the message been paid for.

At 48, the archive matrix is used to determine the price of the email. The matrix, an example of which is shown in FIG. 3, is a cross of storage duration and message size. After the price of the email is determined, the price is inserted into the system's transaction table

together with the email message's system id. The storage duration is determined based upon the default value in the sender's account profile with the third party archiving and verification provider, unless the sender selects a different duration. At 50, a notification is written for each recipient in the email message to an outgoing message queue directory. The notification preferably includes the system message id, the date that the message was archived, and the original contents of the message including all attachments. A sample message is shown in FIG. 26. At 52 the cataloging daemon checks its particular queue and begins processing the next email message.

The email message remains stored with the third party archiving and verification provider for a time determined by the sender's user profile, which was established at the time the sender opened its account, as from time to time amended. Alternatively, the user could be allowed to select the time for storage at the time the message is sent. The user can also extend the time for storage later, as described below. **The third party verification provider preferably provides the sender with access to the stored email messages via a web browser, allowing the sender to manage the stored messages, deleting unneeded messages, extending the storage time for**

messages, and requesting verified copies of messages.[14] The

system and method of the present invention provide a secure

method for Internet users to communicate registered emails on the

Internet without using conventional email clients such as Microsoft's

Outlook Express or Netscape's Network Navigator. Instead,

messages are created and read inside a web browser such as

Microsoft's Internet Explorer, or Netscape's Navigator. Further,

unlike conventional email, the system and method of this invention

allow the sender to know if and when a message has been read.

The system and method allow the sender to see the state of

any message, i.e., the user can see that the message has been

delivered and read by the recipient, in contrast to conventional

email where a user sends a message and is only notified when

and if the recipient replies. According to an alternate aspect of

the invention, the system and method also allows the sender to

receive an electronic or telephone reply to a needed request.

On the FIG. 7 "Main Menu--Welcome" page, the user would click

"gProof Confidential" link, and reach the FIG. 20 page. From the

---

[14] Sykes specification, US publication number 2002/0129108, paragraph

41, line 1, to paragraph 47, line 12, as cited by Examiner in the Final

Office Action, page 5, paragraph 1.

FIG. 20 page, the user the "Outbox" button to reach the FIG. 21 screen. On the FIG. 21 screen, the user is presented with an attachment box, an upload, and next buttons. As the user uploads files, they appear in the attachment box. Thee messages are stored on the system server as MIME entities. This preserves the content-type and other properties needed. The file names are defined as "internalMessageID.count++". After the user clicks the next button, the user is prompted with the "to", "from", "subject", and "body" form. The user is prompted with a confirmation of how much the message will cost and a "Send it" button.

As shown in FIG. 23, at 100, the Sender securely uploads email message to Third Party Archiving and Verification Provider. At 102, Third Party Archiving and Verification Provider emails Recipient that an message <u>is waiting</u>. At 104, <u>Recipient</u> <u>**securely downloads message from Third Party Archiving and**</u> <u>**Verification Provider**</u>. At 106, Third Party Archiving and Verification Provider emails Sender when Recipient receives message.[15]

---

[15] Sykes specification, US publication number 2002/0129108, paragraph 59, line 1, to paragraph 61, line 8.

- The user is able to check the status of the message and view the selection. A time and date stamp can be applied to show when the message was received, and when the selection was made.[16]

2. THE METHOD OF EMAIL "VERIFICATION" IN THE PENDING APPLICATION IS NOT DISCLOSED BY SYKES

In the Office Action, Examiner states[17] Sykes discloses a method and system for archiving, registering, and verifying electronic communications transmitted between clients and recipients via a network (i.e. internet), (abstract and paragraph [0004], lines 1-13). Specifically, Examiner states that Sykes discloses the third party archiving and verification system to comprise: [18]

- The method for registering and certifying an electronic message, the system and method further comprising a client, an intended recipient, a website (i.e. third party archiving and verification website, Figures 4-22), a processing unit (i.e. third party archiving and verification server), an email database, **a means (i.e. third party archiving and verification provider) to register the electronic message, the system and method,** (abstract;

---

[16] Sykes specification, US publication number 2002/0129108, paragraph 65, line 9 to line 13, as cited by Examiner.

[17] Application/Control Number 09/982,145, Office Action, pp 6-8.

[18] Application/Control Number 09/982,145, Office Action, pp 6-8.

paragraph [0004], lines 1-13; and paragraph [0038], line 1 to paragraph [0040], line 17), comprising the steps of:

- The client accessing the website and establishing a registration account; the processing unit assigning a code (i.e. account ID) to the registration account of the client, (paragraph [0048], line 1 to paragraph [0049], line 16 and Figure 4); and

- The processing unit receiving the electronic message, the electronic message being from the client; the processing unit storing information about the electronic message and the registration account in the email database; the processing unit resending the electronic message to the intended recipient as identified by the client in the registration account; the processing unit tracking the date the electronic message was sent by the processing unit; the processing unit tracking the date the electronic message was received by the intended recipient; **the processing unit creating a confirmation record (i.e. message table entry) that comprises the date the electronic message was sent and the date the electronic message was received by the intended recipient; the processing unit sending the client a copy of the confirmation record (Figure 26)**; and the processing unit storing information

about the confirmation record and the registration account in the email database, (paragraph [0038], line 1 to [0047], line 12; paragraph [0059], line 1 to paragraph [0061], line 8; and paragraph [0065], lines 9-13).

Applicant argues that the above cited "verification" method Examiner states is disclosed in Sykes is not analogous to the method disclosed in the PENDING application, as amended in the second response to the Final Office Action. In fact, Applicant notes that the references to Sykes, as cited by the Examiner, reads precisely as follow in the Sykes specification:

- A method and system for archiving and/or **verifying electronic communications.** The method and system provide verification of an email sent by a sender to a recipient, comprising receiving a copy of an email as an addressee; indexing the email according to at least one of sender, recipient, date, or subject matter; **and storing an exact copy of the email as received**. The method and system also provide for secure electronic communication between a sender and at least one recipient, comprising receiving from the sender view a secure internet connection a message and the email address of at least one intended recipient of the message; sending an email message to the at least one intended recipient of the message that a message is waiting; transmitting the message to

the at least one intended recipient via a secure internet connection established by the at least one intended recipient; and sending an email message to the sender that the at least one recipient has been sent the message. [19]

- This invention relates to archiving and/or verifying electronic communications. According to a first aspect of the invention relating to sending verifiable email messages, the invention comprises **addressing the email to a third party verification provider, either as an addressee or as a cc, who will index the message according to at least one of sender, date, recipient, and subject, and store an exact copy of the e-mail message.** Similarly, the invention also relates to providing **email verification** of an email sent by a sender to a recipient, **comprising receiving a copy of an email as an addressee; indexing the email according to at least one of sender, recipient, date, or subject matter; and storing an exact copy of the email as received.**[20]

- According to a first aspect, this invention relates to a **system and a method for senders to backup and archive email to a third party server without the need for conventional backup**

---

[19] Sykes abstract, US publication number 2002/0129108, as cited by Examiner.

[20] Sykes specification, US publication number 2002/0129108, as cited by Examiner.

software, thereby providing proof of on-line communications. The system and method are preferably implemented by a third party archiving and verification provider using an Application Service Provider ("ASP") model that allows a sender to use the system and method regardless of his or her location on the Internet. An example of the structure of tables in a SQL database for implementing the system and method of this invention is shown in Appendix A, attached hereto, and incorporated herein by reference. In the preferred embodiment, no special software is required, and an email sender can use the system without changing his standard email process.

- Referring to FIG. 1, at 22 the sender sends an email to the recipient, and to the third party archiving and verification provider either as an addressee (via the "To:" field) or as a copy (via the "CC:" field). ... At 24, the email message is received by the third party archiving and verification provider. ... **The email message remains stored with the third party archiving and verification provider for a time determined by the sender's user profile, which was established at the time the sender opened its account, as from time to time amended.** Alternatively, the user could be allowed to select the time for storage at the time the message is sent. The user can also extend the time for storage later, as described below.

Applicant argues that the method of verifying and/or confirming an email message in the PENDING application is not disclosed by Sykes. To state the obvious, the present inventive device, offers archival only as an option for record keeping, and not as a mandatory means of verification of the email itself. As illustrated above, Sykes method of "verification" relies exclusively on archiving an exact copy of the original email for comparison at a future date, if needed. The internal (host computer of the verification and archive provider) verification record (i.e. the copy of the original email) is coupled with the time of submission and delivery of the original mandatory email. The original sender receives an email with the time and date that the email was received from the sender and when it was retrieved by the intended recipient.[21]

More importantly, and perhaps significantly, the method disclosed by Sykes does not verify the "contents" of an email, notwithstanding a "verification record", per the method disclosed in the PENDING application. To verify the content of an original email at a future date, the requesting (authorized) party must request a "notarized" version of the email from the archives of the verification provider as insurance against manipulation by an outside party[22]. In the method disclosed by Applicant's application, the contents of the original email message are contained in the verification record along with the time and date of submission and delivery

---

[22] Sykes specification, US publication number 2002/0129108, FIGS and 10 and 12.

of the email. **Depending on the service verification request, the confirmation record may also include biometric information, and other requested information, such as a birth date or social security number. The contents of the verification record in its entirety are provided to the sender of the original email. The independent third party provider does not retain/archive a copy of the email contents, unless requested to by the original sender of the email.** The only information archived by the independent third party provider is information regarding the time and date of submission and delivery and the code associated with the digital certificate that comprises the verification record. Specifically, the specification of the PENDING application discloses:

- The present invention discloses a system, method and process to facilitate three primary functions as follow below.

- Registered or Certified Email by an independent authority wherein the originator/sender of the electronic mail is identified. Method one is **an independent verification that an electronic mail (including all attachments thereto) was sent to the intended recipient (as identified by the Client) and the time and date of submission (when the electronic mail was sent) and the time and date of delivery to the intended recipient.** Verification is a function of the processing unit who sends the electronic mail independent of the Client, albeit on behalf of the Client, who is identified as the sender/originator of the electronic message. Upon delivery to the

recipient, **the Client shall receive a confirmation of the time and date in the form of a digital certificate;**

- Registered or Certified Email by an independent authority wherein the originator/sender of the electronic mail is anonymous. **Method two is an independent verification that an electronic mail (including all attachments thereto) was sent to the intended recipient (as identified by the Client) and the time and date of submission (when the electronic mail was sent) and the time and date of delivery to the intended recipient.** Verification is a function of the processing unit who sends the electronic mail independent of the Client, albeit on behalf of the Client who is not identified. In this instance, the Processing Unit is identified as the sender of the electronic message only. Upon delivery to the recipient, **the Client shall receive a confirmation of the time and date in the form of a digital certificate;** and

- Registered or Certified Email by an independent authority wherein the originator/sender of the electronic mail requests that the recipient's identity be verified prior to receipt of the electronic mail. **Method three is an independent verification of the recipient's identity (as identified by the Client) by an independent authority prior to the recipient receiving the electronic mail. Per methods one and two above, in this instance, the independent authority (the processing unit) confirms the time**

and date of submission (when the electronic mail was sent)
and the time and date of delivery to the intended recipient.
Verification is a function of the processing unit who sends the
electronic mail independent of the Client, albeit on behalf of the
Client, who may or may not be identified. Upon delivery to the
recipient, the **Client shall receive a confirmation of the time and**
date in the form of a digital certificate, and a confirmation that
the intended recipient's identity was verified before receiving
the electronic mail from the Client.[23]

- The Processing Unit keeps an internal record of the account
request and a copy of the email content (if requested). Upon
personal identity verification, the Processing Unit submits the
electronic message to the intended recipient, as identified by the
Client in the registration account, and tracks the submission and
delivery cycle of the electronic message. The electronic message
indicates whether the Client is the originator of the email or whether
the Processing Unit is sending the electronic message on behalf of
an anonymous entity. **Upon delivery of the electronic message,**
the Processing Unit sends the Client a "Confirmation Record",
typically in the form of a digital certificate, of the time and date
of the submission and of the delivery of the electronic

---

[23] Nassiri specification, US Publication Number 2002/0046250, paragraph
45, line 1 to paragraph 48, line 18.

message. The Confirmation Record further contains the

information used to verify the intended recipient's identity.[24]

As noted above, not only are the verification records of the inventive devices different in substance, but in form. Sykes verification record to the sender of the original email comprises the form of an email with information contained within it. **The verification record of the present inventive device is in the form of a digital certificate that is tamper proof**; hence the distinction that the verification record disclosed by the PENDING application "verifies" the content of the email without the need to utilize the independent third party provider in the future .

Applicant submits that Sykes fails to disclose a method whereby the method of verification is based on information other than an archived record of the original email. As such, Applicant submits that its method is not anticipated by Sykes and is patentable over Sykes.

Applicant submits that Sykes fails to disclose a method whereby the third party provider provides a verification record in the form of a digital certificate. As such, Applicant submits that its method is not anticipated by Sykes and is patentable over Sykes.

---

[24] Nassiri specification, US Publication Number 2002/0046250, paragraph 67, line 1 to line 18.

Applicant submits that Sykes fails to disclose a method whereby the third party provider provides a verification record in the form of a digital certificate that contains personal identity information. As such, Applicant submits that its method is not anticipated by Sykes and is patentable over Sykes.

Applicant submits that Sykes fails to disclose a method whereby the third party provider provides a verification record in the form of a digital certificate that contains biometric information. As such, Applicant submits that its method is not anticipated by Sykes is patentable over Sykes.

3. THE METHOD OF THE PROCESSING UNIT (INDEPENDENT THIRD PARTY VERIFICATION) IN THE PENDING APPLICATION IS NOT DISCLOSED BY SYKES

Applicant submits that the purpose and function of the independent third party verification provider in the PENDING application and that disclosed by Sykes are fundamentally distinct. In the PENDING application, the third party verification provider (in addition to being accessible via a website) comprises an actual physical place of business that can be accessed for the services disclosed in the specification: namely, a registered or certified email request, an anonymous registered or certified email request, or a request for identity verification of an intended recipient. With respect to the latter request, maintaining a physical presence is of the utmost importance in the event that the intended recipient be required to provide either original hard copy personal identity identification, or to

provide biometrics as a proof of identity prior to receiving the intended email. Specifically, the method of the PENDING application discloses:

- **A request for identity verification prior to the receipt of registered or certified mail entails the Processing Unit contacting the intended recipient prior to sending the electronic message, and any attachments thereto**. The Processing Unit verifies that the email account to which the electronic message is to be routed corresponds to the identity of an intended recipient, prior to sending the electronic message. Alternatively, the Processing Unit may hold an electronic message on behalf of the sender, **whereby the intended recipient is verified in person at a service center maintained by the present invention**. Upon verification of the recipient's identity, the Processing Unit notifies the Client of when the electronic message was delivered to the intended recipient. Notification typically comprises a digital certificate that is emailed to the Client. If requested, the processing Unit retains a copy of the message contents, including any attachments, for future reference. In any event, the Processing Unit retains a record of the time and date the message was sent and when it was delivered for future reference.[25]

- Registered or Certified Email by an independent authority **wherein the originator/sender of the electronic mail requests that the recipient's**

---

[25] Nassiri specification, US Publication Number 2002/0046250, paragraph 29, line 1 to line 20.

identity be verified prior to receipt of the electronic mail. Method three is an independent verification of the recipient's identity (as identified by the Client) by an independent authority prior to the recipient receiving the electronic mail. Per methods one and two above, in this instance, the independent authority (the processing unit) confirms the time and date of submission (when the electronic mail was sent) and the time and date of delivery to the intended recipient. Verification is a function of the processing unit who sends the electronic mail independent of the Client, albeit on behalf of the Client, who may or may not be identified. Upon delivery to the recipient, the Client shall receive a confirmation of the time and date in the form of a digital certificate, and a confirmation that the intended recipient's identity was verified before receiving the electronic mail from the Client.[26]

- The Client selects the appropriate service by way of a pull down menu on the website with the available options: registered mail, certified mail, return receipt mail, delivery confirmation, submission confirmation, and the like, along with a request for Identity Verification. Identity shall be established by criteria selected by the sender using a pull down menu on the website. The recipient's identity may be verified by:

   (i) having the intended recipient using a predetermined electronic code provided by the Client; or

---

[26] Nassiri specification, US Publication Number 2002/0046250, paragraph 48, line 1 to line 18.

(ii) having the intended recipient using a predetermined electronic code provided by the Processing Unit;

(iii) having the intended recipient go to a Processing Unit service center for an in-person verification using the intended recipient's personal identification, including, but not limited to, personal paperwork such as a birth certificate, a passport, a driver's license and the like; or

(iv) having the intended recipient provide bio-metric verification; or

(v) other means whereby the intended recipient utilizes a predetermined code, a password or other means of encryption.[27]

- "Identity Verification" denotes a variety of services offered by the inventive device. The services may comprise, but are not limited to, verification using digital certificates, biometric information such as a thumbprint, voiceprint, retinal scan, a graphical, hand written signature, or personal identity papers such as a drivers license, a passport, and the like.[28]

In contrast, the method disclosed by Sykes fails to disclose any method of identity verification prior to an intended recipient being allowed to access its website to download the waiting email. The method of Sykes fails to disclose the ability of the sender to independently request that the recipient be identified by

---

[27] Nassiri specification, US Publication Number 2002/0046250, paragraph 58, line 1, to paragraph 63, line 3.

[28] Nassiri specification, US Publication Number 2002/0046250, paragraph 84, line 1 to line 7.

either personal identity documents or biometric information. In fact, the method disclosed by Sykes is incapable of providing any identification verification services as a priori to receiving the email. In fact, the method disclosed by Sykes only verifies that the intended recipient's email address is registered in order to gain access to the website to download the email being held for the intended recipient. Specifically, the method of Sykes discloses:

- Where the recipient does not have an account with the Third Party Archiving and Verification Provider, the system and method can include a verification system to make sure that the message is delivered to the proper recipient. As described above, when the sender clicks the "Confirm" button on the FIG. 21 page, the system checks to see if the addressee in the "To:" has an account with the Third Party Archiving and Verification Provider. If the recipient does not have an account, the system sends an email that instructs the user to go to Third Party Archiving and Verification Provider's website and create an account. After the recipient creates an account, with the Third Party Archiving and Verification Provider's website, the system generates a 64 character string that relates to that user's email address. The system then sends an email to that address with the 64 character ID embedded in a link. When recipient clicks on that link, the system verifies that the recipient's email address is valid because they referenced an ID that was sent to that email address. The same ID is mapped to the same address in the Third Party Archiving and Verification Provider's database. After the user clicks the link, the

Third Party Archiving and Verification Provider's system marks the recipient's account as active, then searches the database for any email messages that do not yet have an ID assigned to it, and which also have the recipient's email address in the "To:" line. After the system finds the email messages meeting these criteria, the messages are then assigned to that userID. Thus when the recipient logs in for the first time, the message or messages addressed to the recipient will be waiting for the recipient.[29]

Moreover, there exist fundamental issues between the method disclosed in Sykes and the present inventive device with respect to access to the archived records and management of the archived records. The method disclosed in the PENDING application does not permit retrieval of archival records by outside parties, or manipulation of archived records by outside parties. Management and control of the verification records is controlled by the independent third party provider, and access (i.e. requesting a copy of the archived confirmation record) is restricted to the original client that tendered the service request, or an authorized third party, as designated by the independent third party provider. In contrast, the method disclosed by Sykes allows the originator of the email to access the archived files, and to manipulate the archived files according to the needs of the account holder. Specifically, Sykes discloses a method whereby:

---

[29] Sykes specification, US publication number 2002/0129108, paragraph 63, line 1 to line 30.

- **The third party verification provider preferably provides the sender with access to the stored email messages via a web browser, allowing the sender to manage the stored messages, deleting unneeded messages, extending the storage time for messages, and requesting verified copies of messages.**[30]

- The system and method of the present invention provide a secure method for Internet users to communicate registered emails on the Internet without using conventional email clients such as Microsoft's Outlook Express or Netscape's Network Navigator. Instead, messages are created and read inside a web browser such as Microsoft's Internet Explorer, or Netscape's Navigator. Further, unlike conventional email, the system and method of this invention allow the sender to know if and when a message has been read. **The system and method allow the sender to see the state of any message, i.e., the user can see that the message has been delivered and read by the recipient, in contrast to conventional email where a user sends a message and is only notified when and if the recipient replies.**[31]

---

[30] Sykes specification, US publication number 2002/0129108, paragraph 47, line 8, to line 12.

[31] Sykes specification, US publication number 2002/0129108, paragraph 59, line 1 to line 14.

Applicant submits that Sykes fails to disclose a method whereby the independent third party provider provides a verification of identity as a priori to the intended recipient receiving the email. As such, Applicant submits that its method is not anticipated by Sykes and that claim 1 is patentable over Sykes.

Applicant submits that Sykes fails to disclose a method whereby the independent third party provider maintains exclusive control and dominion over the archived confirmation records. As such, Applicant submits that its method is not anticipated by Sykes is patentable over Sykes.

CLAIMS 46-48 AND 50-52 IN VIEW OF SYKES, BYRD AND EPSTEIN

Examiner cites that:

Sykes discloses a method and system for <u>verifying the identity of an intended recipient</u> of an electronic message, in order to facilitate secure communication between clients and recipients via a network (i.e. internet), (abstract and paragraph [0005], lines 1-22). Examiner states that Sykes discloses the third party archiving and verification provider system to comprise[32]:

- A system and method for registering and certifying an electronic message, the system and method further comprising a client, an intended

---

[32] Application/Control No. 09/982,145, Final Office Action, page 9, paragraph 2, to page 11, paragraph 2.

recipient, a website (i.e. third party archiving and verification website, Figures 4-22), a processing unit (i.e. third party archiving and verification server), an email database, a means (i.e. third party archiving and verification server) to register the electronic message, the system and method, (abstract; paragraph [0004], lines 1-13; and paragraph [0038], line to paragraph [0040], line 17), comprising the steps of:

> The client accessing the website and establishing a registration account; the processing unit assigning a code (i.e. account ID) to the registration account of the client, (paragraph [0048], line 1 to paragraph [0049], line 16 and Figure 4);

- The processing unit receiving the electronic message, the electronic message being from the client; the processing unit storing information about the electronic message and the registration account in the email database; the processing unit resending the electronic message to the intended recipient as identified by the client in the registration account; the processing unit tracking the date the electronic message was sent by the processing unit; the processing unit tracking the date the electronic message was received by the intended recipient; the processing unit creating a confirmation record (i.e. message table entry) that comprises the date the electronic message was sent and the date the electronic message was received by the intended recipient; the

processing unit sending the client a copy of the confirmation record

(Figure 26); and the processing unit storing information about the

confirmation record and the registration account in the email

database, (paragraph [0038], line 1 to [0047], line 12; paragraph

[0059], line 1 to paragraph [0061], line S; and paragraph [0065],

lines 9-13); and

- The processing unit notifying the intended recipient that the

processing unit is holding the electronic message pending

verification of the identity of the intended recipient; obtaining

verification information of the identity of the intended recipient,

(paragraph [0005], lines 1-22; and paragraph [0063], lines 1-30).

Applicant respectfully traverses. With respect to identity confirmation as

disclosed by Sykes, (as cited by the Examiner above (paragraph [0005], lines 1-

22; and paragraph [0063], lines 1-30)) Sykes specifically discloses:

- According to a second aspect of the invention relating to

secure electronic communication, the invention **comprises**

transmitting to a third party via a secure internet

connection a message and the email address of at least

one intended recipient of the message, who will <u>send an</u>

<u>email message to the intended recipient indicating that a</u>

<u>message is waiting for the intended recipient</u> via a

secure internet connection, transmit the message to the

<u>intended recipient who establishes a secure internet</u>

<u>connection with the third party, and sends an email to</u>

<u>the sender when the message has been transmitted to</u>

<u>an intended recipient</u>. Similarly, the invention relates to

providing secure electronic communication between a

sender and at least one recipient, comprising receiving from

the sender view a secure internet connection a message and

the email address of at least one intended recipient of the

message; sending an email message to the at least one

intended recipient of the message that a message is waiting;

transmitting the message to the at least one intended

recipient via a secure internet connection established by the

at least one intended recipient; and sending an email

message to the sender that the at least one recipient has

been sent the message.[33]

- **Where the recipient does not have an account with the
  Third Party Archiving and Verification Provider, the
  system and method can include <u>a verification system to
  make sure that the message is delivered to the proper
  recipient</u>. As described above, when the sender clicks
  the "Confirm" button on the FIG. 21 page, <u>the system</u>**

---

[33] Sykes specification, US publication number 2002/0129108, paragraph 5, line 11 to line 22.

<u>checks to see if the addressee in the "To:" has an account with the Third Party Archiving and Verification Provider.</u> If the recipient does not have an account, the system sends an email that instructs the user to go to Third Party Archiving and Verification Provider's website and create an account. **After the recipient creates an account, with the Third Party Archiving and Verification Provider's website, the system generates a 64 character string that** <u>relates to that user's email address</u>**. The system then sends an email to that address with the 64 character ID embedded in a link. When recipient clicks on that link, the system verifies that the recipient's email address is valid because they referenced an ID that was sent to that email address.** The same ID is mapped to the same address in the Third Party Archiving and Verification Provider's database. **After the user clicks the link, the Third Party Archiving and Verification Provider's system marks the recipient's account as active,** then searches the database for any email messages that do not yet have an ID assigned to it, and which also have the recipient's email address in the "To:" line. After the system finds the email messages meeting these criteria, the messages are then assigned to that userID. Thus when the recipient logs in

for the first time, the message or messages addressed to the

recipient will be waiting for the recipient.[34]

Applicant submits that Sykes, as amended, fails to disclose the following

method as disclosed in Applicant's specification. As referenced above, **the**

method of Sykes' discloses a method of identifying an email

address, not the intended recipient, per the method disclosed in the

PENDING application. Essentially, "verification" according to the method

entails registering with the inventive device to receive email that is being

held for the recipient. Once verifying that an email address is registered

with the Third Party Archiving and Verification Provider's system, the

system marks the recipient's account as "active", thereby "verifying" the

recipient.

Applicant submits that verifying that an email address was registered with

the third party provider does not constitute verifying the identity of the of

the intended recipient, as disclosed by the method of the PENDING

application. Applicant's specification and claims, as amended, further

specify that the step of verifying an intended recipient's email address is

not achieved by the intended recipient simply registering with the third

party provider and providing an email address, per the method disclosed

in Sykes. Rather, the intended recipient must provide some form of

---

[34] Sykes specification, US publication number 2002/0129108, paragraph 63
line 11 to line 30.

identification to verify the individual as opposed to the email address (FIG 3)[35].

Specifically, the method of the PENDING application discloses:

- A request for identity verification prior to the receipt of registered or certified mail entails the Processing Unit contacting the intended recipient prior to sending the electronic message, and any attachments thereto. The Processing Unit verifies that **the email account to which the electronic message is to be routed corresponds to the identity of an intended recipient**, prior to sending the electronic message. Alternatively, the Processing Unit may hold an electronic message on behalf of the sender, **whereby the intended recipient is verified in person at a service center maintained by the present invention**. Upon verification of the recipient's identity, the Processing Unit notifies the Client of when the electronic message was delivered to the intended recipient. Notification typically comprises a digital certificate that is emailed to the Client. If requested, the processing Unit retains a copy of the message contents, including any attachments, for future reference. In any event, the Processing Unit retains a record of the time and date the message was sent and when it was delivered for future

---

[35] Nassiri specification, US Publication Number 2002/0046250, paragraph

reference.[36]

and

- With reference to FIG. 3, **the Client may request to have the identity of the intended recipient confirmed** prior to the recipient receiving the electronic mail. Per the method depicted in FIG. 1, the Client must register with the Processing Unit to use the service of its choice on the website. The Processing Unit assigns an identification number or code and a password that corresponds to the registration account for future use by the Client and for the tracking of service requests. Upon registration, the Client may submit an identity verification request, along with a registered or certified email request, should the Client require both services.

- The Client selects the appropriate service by way of a pull down menu on the website with the available options: registered mail, certified mail, return receipt mail, delivery confirmation, submission confirmation, and the like, along with a request for Identity Verification. **Identity shall be established by criteria selected by the sender using a pull down menu on the website. The recipient's identity may be verified by:**

- **(i) having the intended recipient using a predetermined electronic code provided by the Client; or**

---

[36] Nassiri specification, US Publication Number 2002/0046250, paragraph 29, line 1 to 20.

- (ii) having the intended recipient using a predetermined electronic code provided by the Processing Unit;

- (iii) having the intended recipient go to a Processing Unit service center for an in-person verification using the intended recipient's personal identification, including, but not limited to, personal paperwork such as a birth certificate, a passport, a driver's license and the like; or

- (iv) having the intended recipient provide bio-metric verification; or

- (v) other means whereby the intended recipient utilizes a predetermined code, a password or other means of encryption.[37]
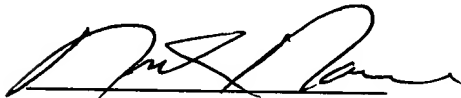
---

[37] Nassiri specification, US Publication Number 2002/0046250, paragraph 51, line 11, to paragraph 63, line 3.

CONCLUSION

Applicant submits that the stated grounds of rejection in the pending claims have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider and withdraw the presently outstanding rejections. It is believed that a full and complete response has been made to the outstanding Office action, and as such, the present application is in condition for allowance. Thus, prompt and favorable consideration of this amendment is respectfully requested.

Respectfully Submitted this day of August 3rd, 2007:

Nick Nassiri